安天周观察

主办：安天　2017 年 2 月 20 日（总第 76 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天收到黑龙江省委网信办感谢信

近日，黑龙江省委网络安全和信息化领导小组办公室（以下简称“黑龙江省委网信办”）向安天发来感谢信，感谢安天对 2016 年黑龙江省网络安全检查工作、2016 年黑龙江省网络安全宣传周活动的积极参与和配合。

2016 年 11 月，由黑龙江省委网信办组织实施的网络安全检查工作中，安天派出多位网络安全专家，发挥安天专业优势，准确排查网站安全隐患和漏洞等工作，完成了对多家单位在网络安全管理、关键信息基础设施等多方面的考核，获得受检单位的认可和好评。

2016 年 9 月 19-25 日，在“2016 年黑龙江省网络安全宣传周活动”期间，安天作为协办单位，举办了反病毒专题展览活动。同时，安天工程师还在网络安全宣传周期间举办了多场专题技术培训，受到了各方一致好评。

黑龙江省委网信办在感谢信中提到，“安天为提升黑龙江省党政机关网络安全防护能力做出了不懈的努力”、“为成功举办网络安全宣传周提供了重要保障”。

作为起步于哈尔滨的企业，安天一直坚持“扎根龙江，辐射全国、放眼世界”的宗旨。安天始终专注于威胁检测领域，在地方政府的支持下，凭借自身的技术实力、技术展现力和技术文化，安天已经成为龙江一张独有特色的高科技名片。安天也一直积极参与省内信息安全建设相关项目。在黑龙江省委网信办的指导下，安天承建了由黑龙江省委网信办组织建设的黑龙江省网络安全态势感知和应急处置平台，平台具备监测全省网站系统的安全漏洞能力，尤其是以党政机关网站及其它以互联网基础设施为重点监测对象，具备监测全省移动终端、恶意代码感染状况的能力；具备针对重点单位通过流量采集分析监测各类威胁事件的能力。该平台由安天态势感知相关产品组成，综合传统 PC 安全及新型的移动安全，全天候、全方位感知网络安全态势，建立和完善了网站和重要信息系统的安全监测、预警、应急处置管理机制，同时具备流量威胁感知、终端威胁感知和深度分析的能力，有效实现了“威胁与隐患统一发现、提早预警、快速处置”的目标，为全省网络环境初步建立了牢固的安全防线。

经过 17 年的发展，安天的技术实力已多次得到相关主管机构的认可，基于安天探海、智甲、追影、态势感知等产品的安全服务能力曾多次收到来自行业主管部门和用户的书面感谢。

安天参展 RSA2017 安全大会

近日，一年一度的美国 RSA 大会在旧金山拉开帷幕。RSA 像是网络安全产业的“万国博览会”，也是洞察安全产业发展方向的一个窗口。这是安天连续第七次作为展商参加 RSA 大会。

今年的 RSA 大会主题是：POWER OF OPPORTUNITY，更让我们感到，我们要把握机遇，积蓄力量，才会在网络安全的赛场上厚积薄发，才能在充满机会的时代，不沦为机会主义者。安天今年在北展馆设立双展台（北展馆 5010 和 5012）。

安天以“安天实验室和 AVL Mobile Security”双品牌同时亮相，展示安天基础感知分析体系和安全生态所支撑下一代威胁检测引擎、深度分析能力和威胁情报服务，体现了安天技术布局和继续发力国际市场的决心。

本次大会，安天重点关注安全基础能力改进、流量和端点检测的新进展和威胁情报的有效落地。

一周简讯

- 安天联合电信云堤深度揭秘银行木马 DMB
- 安全厂商曝光针对沙特的魔术犬 APT 攻击行动
- 研究人员利用 JavaScript 绕过 ASLR 安全机制
- 劫持医疗设备恶意代码 MEDJACK 新变种被发现
- Win10 移动 OS 被发现绕过锁屏访问图片库 Bug
- APT28 组织 X-Agent 后门被发现首个 Mac 版本
- WordPress REST API 漏洞被攻击者用于安装后门

安天 CERT 整理，详情请见 http://bbs.antiy.cn

安天移动安全 & 中国电信云堤联合发布报告《Dark Mobile Bank 之钓鱼篇》

近日，安天移动安全 & 中国电信云堤联合发布报告《Dark Mobile Bank 之钓鱼篇》（以下简称报告），报告数据以 AVL Insight 移动威胁情报平台为基础，针对“网络钓鱼”非法活动做了系统专业的调研和分析。

通过《报告》可以预见的是，在之后数年移动网络安全依然不容乐观，隐私泄露和移动攻击的泛滥和融合还会进一步加深，带来欺诈泛滥成灾，导致网络攻击威胁泛滥并进一步的加深。（报告地址：http://blog.avlsec.com/2017/02/4445/dark-mobile-bank/）

每周安全事件

类 型	内 容
中文标题	研究人员发现散播 Shamoon 恶意软件的 Web 服务器
英文标题	Revealed：Web servers used by disk-nuking Shamoon cyberweapon
作者及单位	The Register；Iain Thomson
内容概述	近日，研究人员已经发现并确定了用来散播 Shamoon 的服务器。 Shamoon 恶意软件于 2012 年浮出水面，当时感染了全球最大石油生产公司沙特阿美 (Saudi Aramco)3 万个工作站，擦除了硬盘数据，使沙特阿美陷入恐慌。自那之后，攻击者不断完善该恶意软件，持续攻击沙特政府和行业的高价值目标，最近一次攻击发生在不久前。 目前，有关研究人员认为，他们已经破解了 Shamoon 操作人员使用的传播技术。研究人员可能知道攻击者如何让恶意软件进入系统，这为 IT 经理提供绝佳机会，以便 IT 经理在 Shamoon 破坏数据之前发现是否存在感染问题。
链接地址	https://www.theregister.co.uk/2017/02/16/researchers_catch_drivedestroying_domains_for_cyberwar_shamoon_malware/

每周值得关注的恶意代码信息

经安天检测分析，本周有 10 个移动平台恶意代码和 4 个 PC 平台的恶意代码值得关注

平台分类	关注方面	名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.spynote.a[prv，exp，rmt]2017-02-12	该应用程序运行时，会在后台上传设备信息，获取远程控制指令，根据远程控制指令可以上传用户的短信、联系人信息、通话记录、浏览器书签、GPS 地理位置信息。并执行后台录音、后台删除或者插入短信及联系人信息、远程控制发送短信、拨打电话、后台推送应用等操作。会造成用户的隐私泄露和资源消耗，建议立即删除。（威胁等级高）
		Trojan/Android.Charger.a[prv，exp] 2017-02-13	该应用伪装成其他应用，运行后会申请激活设备管理器，如果得到授权，则进行锁屏勒索并窃取用户设备上的联系人和短信，造成用户隐私泄露资费损耗，建议立即卸载。（威胁等级高）
		RiskWare/Android.payplug.a[exp，pay]2017-02-15	该应用安装后无图标显示，捆绑多种支付插件，包含风险代码，造成资费损耗，建议卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.HiddenAds.be[exp，prv]	该应用伪装成 Google Play Games，运行后会删除自身图标，收集并上传固件信息，同时包含广告插件。会造成用户隐私泄露、资费消耗，建议卸载。（威胁等级高）
		G-Ware/Android.jianmo.bs[rog，sys]	该程序运行后会在界面置顶，勒索用户添加指定 QQ 进行付费解锁，造成用户资费损失，建议不要安装。（威胁等级低）
		PornWare/Android.E4Asexplayer.j[rog，exp]	该应用为 E4A 开发的色情播放器，运行后会诱导用户点击付费下载，造成用户资费损耗，建议使用绿色健康软件。（威胁等级低）
		Trojan/Android.SmsThief.be[prv]	该应用伪装成 Flash Player，程序运行会监听短信，获取短信信息并连网上传，造成用户隐私泄露。（威胁等级高）
		Trojan/Android.FakeApp.db[exp]	该应用会伪装成手机百度，程序运行后会启动浏览器访问指定网址，再桌面安装快捷图标，判断是否安装相关组件并启动。会私自下载造成用户资费消耗。（威胁等级高）
		RiskWare/Android.Rootnik.v[exp]	该程序包含风险代码，下载子包动态加载，私自提权，警惕该程序下载安装未知程序造成用户资费损耗。（威胁等级低）
		Tool/Android.SMSBomber.w[exp]	该应用为短信轰炸机程序，供用户实施对指定目标进行短信轰炸，请谨慎使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability	Microsoft Office Memory Corruption Vulnerability - CVE-2016-7193 Microsoft Office 容易出现远程代码执行漏洞。攻击者可以利用此问题在受影响的应用程序的上下文中执行任意代码。尝试漏洞失败会导致拒绝服务攻击。（威胁等级高）
	较为活跃的样本	Trojan/Win32.Shifu	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后连接远程服务器，收集系统信息（尤其是银行相关信息）并回传。（威胁等级高）
		Worm/Win32.Gamarue	此威胁是一通过电子邮件传播的可以窃取用户信息的蠕虫家族。该家族样本运行后连接远程服务器接受攻击者操作，收集系统敏感信息回传，通过邮件附件进行传播。（威胁等级高）
		Trojan[Ransom]/Win32.Crysis	此威胁是一类加密用户文件以勒索金钱的木马家族。该家族样本运行后会加密多种格式文件，收集系统信息，与加密 ID 一同回传给攻击者。（威胁等级中）

Mirai 开始攻击 Windows 系统

John Leyden / 文　安天公益翻译小组 / 译

近日，相关安全人员发现劫持了数十万物联网设备的 Mirai 恶意软件现在也能够感染 Windows 系统了。

Mirai 是在 2016 年 8 月被发现的，它感染了全球大量不安全的 Linux 设备，并对目标 (主要是 DNS 提供商 Dyn) 发起 DDoS 攻击。许多家庭用户依赖 Dyn 的服务器来支持他们的网站和在线服务。

在 2016 年 10 月的攻击中，很多网站和服务被迫下线，导致大量用户无法上网。

受影响的设备包括很多个人数字录像机，网络摄像头等。Mirai 扫描具有开放端口的机器，然后使用默认或硬编码的密码登录，从而控制这些机器。

近期，俄罗斯安全软件制造商 Dr Web 的研究人员发现了 Mirai 僵尸程序的 Windows 版本，该版本首先感染微软主机，然后扫描存在漏洞的物联网设备。这意味着，如果公司网络上的 Windows 客户端和服务器遭到感染，则相邻的存在漏洞的设备也会遭到攻击。

该 Windows 版本用 C++ 编写，被命名为 Trojan.Mirai.1，它使用 IP 地址和密码列表来扫描网络中的设备并尝试登录这些设备。

如果 Trojan.Mirai.1 通过 Telnet 进入 Linux 机器，就会在受感染的机器上下载并运行 Linux.Mirai，从而继续传播。

如果它在网络上找到了 Windows 机器，就会利用 WMI(Windows 管理规范) 和 IPC(进程间通信) 在计算机上启动一个新的进程来感染它，从而继续传播。

2017 年 1 月底，研究人员首次在微软系统上发现了 Mirai，它使用 MS SQL Server 事件服务，作为管理员执行命令并安装恶意软件。

该木马如何在公司网络上创建据点呢？这取决于它的主要工具，例如，利用电子邮件附件作为诱饵。如果你的 Windows PC 和服务器被未经授权的软件感染，你最先想到的可能是你的物联网设备。话虽如此，该恶意软件只需要成功感染一个或两个 Windows 机器，就能够在企业的 Linux 设备中传播。

加利福尼亚州 DDoS 缓解公司 Nsfocus IB 的技术专家理查德·麦尤斯 (Richard Meeus) 说，Mirai 的最新变种对企业带来了更大的风险。

麦尤斯说：“Mirai 能够利用 Windows 机器传播意味着，它已经建立了一个进入私人网络的途径。以前，我们认为没有直接连网的物联网设备面临的风险不那么大。鉴于许多家庭和企业都在使用 Windows 设备，Mirai 现在能够感染更多的设备了。”

原文名称	Lovely. Now someone's ported IoT-menacing Mirai to Windows boxes
作者简介	John Leyden，The Register 记者，主要关注安全领域。
原文信息	2017 年 2 月 10 日发布于《The Register》 原文地址 https://www.theregister.co.uk/2017/02/10/windows_mirai_bot/
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

安天发布《僵尸网络 Dklkt 家族分析》

近日，安天追影团队通过僵尸网络监控捕获到一个由 Windows 远控代码演化的 Linux 恶意代码家族。经过详细分析，确认其是名为 Dklkt 的 DDoS 僵尸网络家族。攻击者将 Windows 平台的 Gh0st 系列远控程序源码，改编为在 Linux 平台上运行的特殊版本。Dklkt 是 Gh0st 家族进军 Linux 操作系统的典型代表。

经过对样本逆向分析得知，Dklkt 主要实现的是 DDoS 攻击，从目前来看，此家族样本并没有完全继承 Windows 系列的 Gh0st 家族功能，也没有实现被控端样本备份及自启动功能，这说明其功能并没有完善，所以目前该家族在互联网上并不活跃，其检测量较少。目前暂时没有捕获到 Dklkt 生成器与控制端，尚无法确认其被控端能否与 Windows 系列的控制端兼容，但可以肯定的是，Dklkt 被控端可以执行常见的多种攻击类型。

通过被控端样本分析得知，Dklkt 主要实现包括：SYN Flood、HTTP Flood、Drv Flood、ICMP Flood、TCP Flood、UDP Flood、CC Flood 这几种 DDoS 攻击方式。样本运行后，首先会获取系统名称、用户名、系统版本、内存、CPU 配置、系统备注等信息作为被控端向命令与控制服务器 (C&C) 发送的首包数据，随后检查运行配置文件或样本中校验是否存 在 ServiceDllName、m_enable_http、Http Address、szGroup、blDelMe、Self Delete、Config、Password、Remark、Version 等参数，被控端执行 C&C 的远程指令类型也比较繁多，包括 Welcome packet、Update itself、Open shell、Exit、Reboot、Turn off the computer、Run an application、Start proxy 等指令类型。

Dklkt 家族从功能和爆发量来说还未形成规模，但因为有 Windows 系列的 Gh0st 做参照、借鉴，如果 Dklkt 逐渐完善，会有危害互联网安全的可能性。安天提醒广大用户，如果发现系统被 Dklkt 感染，因其被控端没有实现自启动功能，所以仅需要找到被控端样本并将其删除执行重启即可，安天追影小组也会对此家族进行持续关注。目前，安天追影产品已经实现了对该家族样本的检出。

木马程序

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述木马程序进行有效检测，以下为其自动形成的分析报告：

文件被网络威胁感知类设备发现，经由 BD 静态分析鉴定器、美国软件交叉索引 (NSRL) 鉴定器、可交换信息 (EXIF) 鉴定器、静态分析鉴定器、动态行为 (默认环境) 鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器将文件判定为木马程序。

根据动态行为 (默认环境) 得出该文件具有以下行为：疑似 ddos flood 流量攻击、获取计算机系统版本。

文件名	Dklkt
文件类型	BinExecute/Linux.ELF
大小	143 KB
MD5	464DC38C776724B9EC931480419DCF64
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[DDoS]/Linux.Dklkt
判定依据	BD 静态分析

◆ 运行环境

操作系统	中标麒麟
内置软件	默认

◆ 危险行为

行为描述	危险等级
疑似 ddos flood 流量攻击	★★★

◆ 其他行为

行为描述	危险等级
获取计算机系统版本	★★

◆ 其他行为

描述	值
File Size	143 kB
File Type	ELF executable
MIME Type	application/octet-stream
CPU Architecture	32 bit
CPU Byte Order	Little endian
Object File Type	Executable file
CPU Type	i386

报告地址：https://antiy.pta.center/_lk/details.html?hash=464DC38C776724B9EC931480419DCF64